Fault attacks on “secure” Smart Card

Jie Ling and Brian King
Department of Electrical and Computer Engineering, Purdue School of Engineering and Technology

Today’s software engineers are faced with the problem of building secure systems from untrustworthy components, which used widely in everyday life. A Smart Card is a popular security token, with applications integrated in many areas including: credit cards, bank cards, cellular communications, electronic cash, banking, satellite TV and Government identifications. Smart cards are often touted as “secure” portable devices. Applications often assume that information (keys) stored on the card will be securely stored, and access control to the information will be properly maintained. Unfortunately, it has been repeatedly proven that Smart Cards are not as secure as they are commonly supposed to be. For example consider the following scenario, you go to restaurant and pay your bill with a Smart Card (type of bank card), when you pay the bill, do you constantly monitor/observe the card as the waiter uses the card? After the waiter takes the card into their possession, it is possible that they continue to swipe your card in a manner to purposely induce faults and record all the faulty/error information outputted. By analyzing the faulty output later off-line they can retrieve all secret keys, and construct a clone of your card, using it for their needs at your expense. This technique, based on fault injections which modify the behavior of the application, is named “Fault Attack”. Fault attacks on Smart Cards may be diverse in nature but successful nevertheless. In this project using fault attack, we have simulated the process of key recovery for both Elliptic Curve Cryptography (ECC) and RSA systems. Our work investigates both attacks and countermeasure to the attacks.

Mentor: Brian King, Department of Electrical and Computer Engineering, Purdue School of Engineering and Technology